CLAIMS

1. Process for automatically discovering the topology and components of an Intranet network, comprising at least one sub network (70...), to which are attached devices (1, 2, ...) complying with TCP/IP protocol, said process running into one particular device (7) being assigned an IP address and comprising the steps of:

- computing a set of sub network configurations to which the IP address of the device could belong;
- using the ICMP layer of said TCP/IP protocol for successively testing and validating said configurations for the purpose of elaborating an extensive description of the network architecture.

2. Process according to claim 1 characterized by the steps of:

- discovering a first sub network having a determined range;
- computing a sequence of potential candidate sub networks of the same size as that said first sub network and being contiguous with said first sub network;
- successively testing and validating by means of the ICMP layer of the TCP/IP protocol each of said potential candidate sub networks.

3. Process according to claim 1 characterized by the steps of:

- discovering a first sub network having a determined range;
- computing a sequence of potential candidate sub networks being contiguous with said first sub network, and having a range being equal to 2^n .
- successively testing and validating by means of the ICMP layer of the TCP/IP protocol each of said potential candidate sub networks.

4. Process according to claim 1 wherein said testing and validation are based on the computation, for each of said configurations, of a first broadcast address (BC1) and a second broadcast address (BC2) which are used for transmitting a ICMP Echo Request.

5. Process according to claim 4 characterized in that said first and second broadcast addresses (BC1, BC2) are computed in accordance with the following formula:

BC1 = IP AND SubnetMask

BC2 = (IP AND SubnetMask) OR (NOT SubnetMask)

where IP represents the Internet Protocol address assigned to said particular device where said process is being run, and the SubnetMask is the value of the mask corresponding to the sub network configuration which is to be tested and validated.

6. Process according to claim 5 characterized in that the validation of the sub network is then followed by the transmission of successive Simple Network Management Protocol (SNMP) requests to the different addresses within the address range of said validated sub network, for the purpose of extracting and gathering information from the devices attached to said validated sub network.

7. Process according to claim 6 characterized in that said SNMP requests accesses the Management Information Base (MIB), and particularly node 1.3.6.1.2. for the purpose of gathering information relevant to the routers attached to the discovered sub networks.

8. Process according to claim 1 characterized in that said particular device receives an IP address by means of a self IP configuration via where the particular device is assigned an IP address and, possibly, the subnet range of the sub network to which it has been attached.

9. Process for discovering the sub network of an Intranet network to which is attached a pluggable device (7), characterized in that said process involves the steps of:

a) initiating (210) a self IP detection step for the purpose of detecting an IP address;

b) computing (220) a first value representative of a first subnet mask ("/n") comprising a prefix with n logical "1", said first subnet mask corresponding to a first sub network to which is likely to belong said IP address;

c) computing (230) for said value a first and second broadcast addresses (BC1; BC2);

d) transmitting (240) an ICMP Echo Request to said first and second broadcast addresses (BC1, BC2);

e) in response to a positive answer received to both said first and second broadcast addresses (BC1, BC2), validating (270) said value as being the effective value of an existing sub network connected to said Intranet.

f) decrementing n by 1 and repeating steps b)-e) for the purpose of testing new values of possible subnet masks.

10. Process according to claim 1 characterized in that said first and second broadcast addresses are computed in accordance with the following formula:

BC1 = IP AND SubnetMask

BC2 = (IP AND SubnetMask) OR (NOT SubnetMask)

where IP represents the Internet Protocol address assigned to said particular device where said process is being run and the SubnetMask is the value of the mask corresponding to the sub network configuration which is to be tested and validated.

11. Process according to claim 1 characterized in that the discovered topology is transmitted to an external server by means of a HTTP or HTTPS request for the purpose of updating an external database.

12. Apparatus for allowing the discovery of a Intranet network comprising at least one sub network; said apparatus being pluggable into said Intranet and further including:

- means for allowing a connection to said at least one sub network;
- means for achieving a self IP configuration and for receiving an IP address;
- means for computing a set of sub network configurations which are likely to be connected to said Intranet;

- means generating ICMP requests for successively testing and validating the different network configurations for the purpose of discovering the sub networks of said network.

13. Apparatus according to claim 12 characterized by:
- means for determining a first value representative of a first subnet mask ("/n") comprising a prefix with n logical "1", said first subnet mask corresponding to a first sub network to which is likely to belong said IP address;
- means for computing a first and second broadcast addresses (BC1; BC2) to said first value;
- means for transmitting an ICMP Echo Request to said first and second broadcast addresses (BC1, BC2);
- means for testing another value representative of a second subnet mask ("/n-1) if said ICMP Echo Requests do not provide any answer; whereby the subnet mask of the particular sub network where said apparatus is plugged can be automatically discovered.

14. Apparatus according to claim 13 characterized in that said first and second broacast addresses are computed in accordance with the following formula:

BC1 = IP AND SubnetMask
BC2 = (IP AND SubnetMask) OR (NOT SubnetMask)

15. An apparatus comprising program code elements for carrying a method as claimed in any of claims 1 to 11.

16. A computer program product comprising computer program code stored on a computer readable storage medium for, when executed on a computer, performing all the steps of anyone of claims 1 to 11.